P1G500935-USA-AC2)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年　２月２８日
出願番号 Application Number: [ST. 10/C]:	特願２００３－０５３１４５ [ＪＰ２００３－０５３１４５]
出願人 Applicant(s):	東芝テック株式会社 株式会社東芝

２００４年　２月　３日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３１０７９１４

【書類名】　特許願
【整理番号】　TEC067
【提出日】　平成15年 2月28日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G06F　3/12
【発明者】
　【住所又は居所】　静岡県三島市南町６番７８号　東芝テック株式会社　三島事業所内
　【氏名】　光冨　俊之
【特許出願人】
　【識別番号】　000003562
　【氏名又は名称】　東芝テック株式会社
【代理人】
　【識別番号】　100090620
　【弁理士】
　【氏名又は名称】　工藤　宣幸
【選任した代理人】
　【識別番号】　100092576
　【弁理士】
　【氏名又は名称】　鎌田　久男
【手数料の表示】
　【予納台帳番号】　013664
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0107421
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　画像形成装置及び暗号キー設定入力方法

【特許請求の範囲】

【請求項１】　入力された画像データに基づいて画像形成する画像形成装置において、

暗号キーの設定時に、ユーザにより入力された暗号キーのキー値を取り込む入力手段と、

ユーザにより予め定められた所定回数入力されたキー値が、それぞれ同一であるか否かの判断をするキー値判断手段と、

上記キー値判断手段が同一であると判断した場合に、上記入力されたキー値を暗号キーとして記憶する不揮発性記憶手段と、

入力された画像データを画像蓄積手段に蓄積する際に、その画像データに対して上記暗号キーを使用して暗号化すると共に、上記画像蓄積手段に蓄積されている暗号化された画像データを読み出す際は、上記暗号化された画像データを復元する暗号化・復元手段と

を備えることを特徴とする画像形成装置。

【請求項２】　上記入力手段が取り込んだ上記キー値を表示すると共に、入力済みのキー値については認識不可能な表示に変換する表示手段を備える請求項１に記載の画像形成装置。

【請求項３】　上記表示手段は、Ｍ桁のキー値をＮ（Ｍ＞Ｎ）桁毎に分割した場合において、あるＮ桁のキー値部分の入力が終わると、そのＮ桁のキー値部分を認識不可能な表示に変換することを特徴とする請求項２に記載の画像形成装置。

【請求項４】　上記キー値の入力、表示を１０進又は１６進表示法に従った桁表記で行なうことを特徴とする請求項１～３のいずれかに記載の画像形成装置。

【請求項５】　入力された画像データを画像蓄積手段に蓄積する際に、その画像データの暗号化に使用する暗号キーを設定入力する暗号キーの設定入力方法

であって、

ユーザにより入力された暗号キーのキー値を入力手段が取り込み、

キー値判断手段がユーザにより予め設定された所定回数入力されたキー値が同一であるか否かの判断し、

上記キー値判断手段が同一であると判断した場合に、上記入力されたキー値を暗号キーとして不揮発性記憶手段に記憶する

ことを特徴とする暗号キー設定入力方法。

【請求項６】　上記入力手段が取り込んだ上記キー値を表示手段が表示すると共に、入力済みのキー値については認識不可能な表示に変換することを特徴とする請求項５に記載の暗号キー設定入力方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、画像形成装置及び暗号キー設定入力方法に関し、入力したデータを蓄積する蓄積手段を有する画像形成装置に適用しうる。

【０００２】

【従来の技術】

従来、画像形成装置（例えば、複写機、ファクシミリ、プリンタ、スキャナ、複合機等）は、入力したデータを装置内の大容量蓄積装置（ＨＤＤ）に蓄積し、蓄積装置から蓄積データを取り出し、その蓄積データに基づいて用紙等に複写して出力する。

【０００３】

そのため、蓄積装置には入力したデータそのものが蓄積されており、例えば、蓄積手段を盗み出した後に、他の装置等を駆使して蓄積されているデータが悪意に取り出され、情報が流出してしまうという情報漏洩の問題がある。特に、機密文書についての機密文書の漏洩が問題とされる。

【０００４】

従来、このような問題を解決するために、次のような手段を行なうことにより機密文書の漏洩を防止していた。

【０００５】

まず、最初の機密文書漏洩防止手段は、例えば、特定の機密文書について、複写機による複写を禁止することで、機密文書の漏洩を防止していた。

【０００６】

次に、また例えば、複写機による文書の複写を許可複写機による文書の複写を行なう場合、複写を許可されたユーザにのみパスワード等を付与して、そのパスワード等に基づいてユーザ認証を行なうことにより、許可されたユーザ以外の者による複写により、複写機内に蓄積された画像情報をアクセスできないようにして、情報の漏洩を防止していた。

【０００７】

そして、下記の特許文献１及び２は、パスワード等の設定入力方法について記載されている。

【０００８】

【特許文献１】

特開２００１－１６６８４３号公報

【０００９】

【特許文献２】

特開平１０－６３６２１号公報

【００１０】

【発明が解決しようとする課題】

しかしながら、上述した機密文書漏洩防止手段によると、それぞれ次のような問題がある。

【００１１】

上述した最初の機密文書漏洩防止手段の場合、特定の機密文書の複写を禁止することにより、社内の人間の手による機密文書の複製品が、社外に漏洩することを防げるが、社内での使用においては、複写機の本来の機能を制限することになり、利便性を損なう。

【００１２】

また、次の機密文書漏洩防止手段は、パスワード等を使用するユーザ認証につ

いては、複写機が通電中は、ユーザ認証プログラムが動作しているため、不正アクセスを防止できるが、複写機が電源オフ中に、内部の蓄積装置（ＨＤＤ）のみ取り外して、他の装置（例えばパソコン）に、そのＨＤＤを接続して、内部情報の解析をされた場合、認証プログラムが効かないため、内部情報は容易に解読される可能性がある。

【００１３】

ところで、例えばファクシミリ等のネットワークを利用する情報通信の分野において、情報通信を行なう場合、伝送路上での情報の漏洩を防ぐため、情報を暗号化して送信することが行われており、この暗号化方式を入力した画像データにも適用し、蓄積装置に書込む画像データをすべて暗号化してから書込むことで蓄積装置が盗まれても、書込まれた画像データが解読できないようにすることができる。

【００１４】

一般的に利用されている暗号化方式は、予め設定された暗号キーを使用するため、蓄積装置内のデータが解読されないためにも、暗号キーも第三者に知られることなく、かつ、どこに暗号キーを格納しているかをも知られないようにすることが望ましい。

【００１５】

しかし、暗号キーの初期設定時や、既に設定登録済みの暗号キーが何らかの原因により消失等した場合には、改めて暗号キーを設定入力する必要があり、この場合には、暗号キーのキー値を正しく入力することが必要となる。間違えて再設定してしまった場合には、既に蓄積されているデータの読み出しが不可能になったり、暗号化処理が正しく行なわれない場合もある。

【００１６】

そのため、入力画像データを蓄積装置に蓄積する際に、暗号化したデータを蓄積する画像形成装置において、暗号化に供する暗号キーの設定入力時に、ユーザにより暗号キーの設定が正しく行なえ得る暗号キー設定入力方法と、その画像形成装置が求められている。

【００１７】

【課題を解決するための手段】

かかる課題を解決するために、第１の本発明の画像形成装置は、入力された画像データに基づいて画像形成する画像形成装置において、暗号キーの設定時に、ユーザにより入力された暗号キーのキー値を取り込む入力手段と、ユーザにより予め定められた所定回数入力されたキー値が、それぞれ同一であるか否かの判断をするキー値判断手段と、キー値判断手段が同一であると判断した場合に、入力されたキー値を暗号キーとして記憶する不揮発性記憶手段と、入力された画像データを画像蓄積手段に蓄積する際に、その画像データに対して暗号キーを使用して暗号化すると共に、画像蓄積手段に蓄積されている暗号化された画像データを読み出す際は、暗号化された画像データを復元する暗号化・復元手段とを備えることを特徴とする。

【００１８】

また、第２の本発明の暗号キー設定入力方法は、入力された画像データを画像蓄積手段に蓄積する際に、その画像データの暗号化に使用する暗号キーを設定入力する暗号キーの設定入力方法であって、ユーザにより入力された暗号キーのキー値を入力手段が取り込み、キー値判断手段がユーザにより予め設定された所定回数入力されたキー値が同一であるか否かの判断し、キー値判断手段が同一であると判断した場合に、入力されたキー値を暗号キーとして不揮発性記憶手段に記憶することを特徴とする。

【００１９】

【発明の実施の形態】

（Ａ）第1の実施形態

以下では、本発明の画像形成装置の第1の実施形態について図面を参照して説明する。

【００２０】

なお、本実施形態は、画像形成装置の一例としてデジタル複写装置（ＤＰＰＣ）を例に挙げて説明するが、入力された画像を蓄積する蓄積手段を有する画像形成装置（例えば、プリンタ、ファクシミリ、複合機等）に広く適用できる。

【００２１】

本実施形態は、入力した画像データを機体個別の暗号キーを使用して暗号化した画像データを大容量蓄積装置（ＨＤＤ）に蓄積する場合であって、初期設定時、又は、何らかの事情により機体個別の暗号キーが消失した時に、ユーザにより、その機体個別の暗号キーを不揮発性メモリ（ＮＶＲＡＭ）に設定入力させる方法について説明する。

【００２２】

（Ａ－１）第１の実施形態の構成

図１は、本実施形態に係るデジタル複写装置の構成ブロックの概略を示すものである。

【００２３】

図１に示すように、本実施形態に係る画像形成装置は、装置全体を制御するシステム制御部１と、原稿をデジタル信号に変換してデジタル信号の画像データを出力するスキャナサブシステム２と、デジタル信号の画像データに基づいて画像を用紙に印刷して出力するプリンタサブシステム４と、用紙ジャム等の画像形成装置の状態を表示したり、ユーザが複写を行うときの各種パラメータや動作モードを入力する制御パネル７とを備えるものである。

【００２４】

スキャナサブシステム２、プリンタサブシステム４及び制御パネル７は、それぞれＣＰＵ２０３、４３及び７４を搭載しており、これらＣＰＵ２０３、４３及び７４は、全体の制御を行うシステム制御部１のシステムＣＰＵ１０とそれぞれシリアルＩＦを介して制御情報を送受信し各ブロックの制御を行なう。

【００２５】

システム制御部１は、図１に示すように、システム制御回路５と、複数の画像データを蓄積できるＨＤＤブロック８０との２つの基板構成を有するものである。

【００２６】

ＨＤＤブロック８０は、大容量蓄積装置（以下ＨＤＤと呼ぶ）８３０と、暗号・復元化回路８１０と、暗号キーメモリ８２０と、ＩＤＥコントローラ８００とを有するものである。

【００２７】

ＨＤＤ８３０は、暗号化回路８１０により暗号化された複数の画像データを蓄積するものである。ＨＤＤ８３０に暗号化した画像データを蓄積する場合の例として、例えば、本実施形態の画像形成装置の場合、複数枚のコピーを行なう際に、画像データを暗号化してＨＤＤ８３０に記憶し、その蓄積した画像データに基づいて複数枚のコピーを実行する場合や、両面コピーを行なう際に、暗号化した画像データをＨＤＤ８３０に記憶し、その蓄積した画像データに基づいて両面コピーを実行する場合や、又用紙の片面につき２ページ文の画像を並べて印刷する２ｉｎ１印刷を実行する場合などがある。

【００２８】

暗号・復元化回路８１０は、画像データの暗号化処理の際、ＩＤＥコントローラ８００を介してページメモリ制御回路３０によって圧縮処理が行なわれた画像データを受け取り、その圧縮された画像データを暗号キーに基づいて暗号化して、暗号化した画像データをＨＤＤ８３０に蓄積するものである。また、暗号・復元化回路８１０は、暗号化された画像データの復元処理の際、ＨＤＤ８３０に蓄積されている暗号化された画像データを読み出し、その暗号化された画像データを暗号キーに基づいて復元して、復元した画像データ（すなわち、元の圧縮された画像データ）をＩＤＥコントローラに与えるものである。

【００２９】

ここで、暗号・復元化回路８１０が行なう暗号・復元化方式は、機体個別の暗号キーを使用して、元のデータを解読不可能な別のデータに変形し、又その暗号キーを使用して、暗号化したデータを元のデータに復元する暗号・復元化方式であれば広く適用できる。この機体個別の暗号キーは、装置製造の際にそれぞれの装置毎に設定された暗号キーである。

【００３０】

暗号キーメモリ８２０は、画像データの暗号化及び復元に使用する暗号キーを記憶する揮発性のメモリである。暗号キーメモリ８２０は、暗号・復元化回路８１０による画像データの暗号化及び復元処理の際に、ＮＶＲＡＭ１４に記憶されている暗号キーを受け取り、電源オン中は暗号キーを記憶し、電源がオフになる

と、その暗号キーを廃棄する記憶手段である。

【００３１】

ＩＤＥコントローラ８００は、システムバス９と、ＨＤＤ８３０と、暗号化回路８１０と、暗号キーメモリ８２０と、システムバス９とのインタフェースである。ＩＤＥコントローラ８００は、システムバス９を介して、ページメモリ制御回路３０から圧縮処理された画像データを受け取り、暗号・復元化回路８１０に与えるものである。また、ＩＤＥコントローラ８００は、暗号・復元化回路８１０により復元された画像データを、システムバス９を介して、ページ制御回路３０に与えるものである。

【００３２】

次に、システム制御回路５の内部構成について説明する。

【００３３】

システム制御回路５は、システムＣＰＵ１０と、メインメモリ１２と、ＲＯＭ１１と、ＮＶＲＡＭ１４と、ページメモリ制御回路３０と、ＬＡＮコントローラ６０とを有するものである。

【００３４】

なお、システムＣＰＵ１０と、メインメモリ１２と、ＲＯＭ１１と、ＮＶＲＡＭ１４とは、ローカルバス１５を介して接続されている。また、システムＣＰＵ１０と、ＨＤＤブロック８０と、ページメモリ制御回路３０と、ＬＡＮコントローラ６０とは、システムバス９を介して接続されている。

【００３５】

ＮＶＲＡＭ１４は、マシン毎の設定値を格納するバッテリでバックアップする不揮発性の記憶手段である。また、ＮＶＲＡＭ１４は、画像データの暗号化に使用される暗号キーを記憶しており、電源オン後、暗号・復元化回路８１０により暗号化又は復元する際に、その記憶している暗号キーを暗号キーメモリ８２０に与えるものである。

【００３６】

システムＣＰＵ１０は、装置全体を制御するものである。システムＣＰＵ１０の詳細な内部構成については後述する。

【００３７】

ＲＯＭ１１は、装置全体を制御する制御プログラムを記憶するものである。ＲＯＭ１１は、電源オン時に所定の規則に従って、システムＣＰＵ１０により記憶している制御プログラムが読み出され、当該制御プログラムによりブート処理がなされる。また、ＲＯＭ１１は、本実施形態の暗号キーの設定入力に係るプログラムも記憶する。

【００３８】

メインメモリ１２は、揮発性のＤＲＡＭで構成されており、電源オン時に、システムＣＰＵ１０がＲＯＭ１１からロードした制御プログラムを、所定の領域に記憶するものである。また、メインメモリ１２は、電源オン中に、記憶した制御プログラムを動作するものである。また、メインメモリ１２は、ユーザにより入力された暗号キー設定に係るキー値を一時的に記憶するものである。

【００３９】

本実施形態では、暗号キー設定に係るキー値を複数回（例えば２回）ユーザに入力してもらい、それらキー値が共に正しい場合には、そのキー値を暗号キーとする。

【００４０】

ページメモリ制御回路３０は、画像データ（デジタル信号）を一時的にページ単位で記憶するものである。ページメモリ制御回路３０は、画像データをページ毎に一時的に記憶するページメモリ３００と、このページメモリ３００を制御するページメモリ制御部３０１とを有する。また、ページメモリ制御回路３０は、要求に応じて、画像データの圧縮処理及び圧縮された画像データの伸長処理が行なうものである。

【００４１】

ＬＡＮコントローラ６０は、図示しないネットワーク上に接続された端末（例えば、パソコン等）と画像形成記憶装置との間での、画像データの送受信をインタフェースするものである。

【００４２】

制御パネル７は、マシンの状態を表示したり又は各種パラメータの情報を表示

するＬＣＤ７０と、ＬＣＤ７０上に配置されるタッチパネル７１と、テンキー（Ｋｅｙ）７２と、複数のＬＥＤ部７３と、これら制御パネル７の各構成を制御するパネルＣＰＵ７４とを有するものである。

【００４３】

本実施形態では、入力手段として、タッチパネル７１及びＫｅｙ７２を備えるものとしたが、ユーザにより入力操作し得る入力手段であれば広く適用できる。

【００４４】

タッチパネル７１及びＫｅｙ７２の入力手段は、初期設定の場合又は何らかの事情により暗号キーがＮＶＲＡＭ１４から消失した場合等に、ユーザが入力した暗号キーのキー値を取り込むものである。この暗号キーが正しいものであるか否かの判断は、暗号キーのキー値を２回以上（本実施形態では２回とする）ユーザに入力してもらい、その１回目のキー値と２回目のキー値との同一性を判断することによる。そして、１回目と２回目とのキー値が同一であれば、そのキー値を暗号キーとし、１回目と２回目とのキー値が異なっていれば、そのキー値に基づく暗号キーを設定せずエラーとする。

【００４５】

ＬＣＤ７０は、ユーザが入力した暗号キーのキー値を表示する表示部である。ＬＣＤ７０は、ユーザにより入力されたキー値を４桁ごとに区切って、その４桁キー値の入力が終了すると、表示していたキー値をアスタリスク「＊」に変換して表示する。これを一般的に表現すると、例えばM桁（Mは１以上の整数）のキー値をN桁（Mは１以上の整数）（Ｍ＞Ｎ）毎に分割した場合において、あるＮ桁のキー値部分の入力が終わると、そのＮ桁のキー値の部分をアスタリスク「＊」に変換表示するということになる。これは、ＬＣＤ７０に表示されたキー値が第三者に盗み見られることを防止するためである。

【００４６】

また、本実施形態ではキー値をアスタリスク「＊」表示に変換することとするが、アスタリスクに限ることなく、入力したキー値を認識不可能な表示に変換できれば、例えば「－」や「＃」や「スペース（空白）」などの表示であってもよい。

【００４７】

次に、上述したシステム制御回路５のシステムＣＰＵ１０の内部構成について説明する。図２は、システムＣＰＵ１０の内部構成ブロック図を示したものである。

【００４８】

図２に示すように、システムＣＰＵ１０は、ＲＯＭ１１の制御プログラムを実行するＣＰＵコア１００と、ローカルバス１５上のメインメモリ１２（ＳＤＲＡＭ）の制御を行うＤＲＡＭコントローラ１０１と、同じくローカルバス１５上のＲＯＭ１１及びＮＶＲＡＭ１４を制御するＲＯＭコントローラ１０２と、ローカルバス１５とＳＤＲＡＭコントローラ１０１とＲＯＭコントローラ１０２とをインタフェースするローカルバスＩ／Ｆ１０３と、装置上の各ブロックから割り込みを入力し、所定の優先度順位に基づいて唯一の割り込みをＣＰＵコア１００に通知する割り込みコントローラ１０４と、スキャナＣＰＵ２０３とプリンタＣＰＵ４３と制御パネルＣＰＵ７４とＣＰＵコア１００とが通信するためのインタフェースをする３チャネルのシリアルＩ／Ｏ（ＳＩＯ）１０５と、システムバス９上の各ブロックとシステム制御部１上の各ブロックとをインタフェースするシステムバスコントローラ１０６と、タイマー１０７と、ＣＰＵコア１００とこれらシステムＣＰＵ１０の各ブロック（ＤＲＡＭコントローラ１０１、ＲＯＭコントローラ１０２、割り込みコントローラ１０４、３チャネルのシリアルＩ／Ｏ（ＳＩＯ）１０５、システムバスコントローラ１０６、タイマー１０７）とを接続する内部バス１０８とを有するものである。

【００４９】

次に、上述したページメモリ制御回路３０のページメモリ制御部３０１の内部構成について説明する。図３は、ページメモリ制御部３０１の内部構成を示すものである。

【００５０】

図３に示すように、ページメモリ制御部３０１は、内部の各ブロックとシステムバス９とのインタフェースを行うシステムバスインタフェース（システムバスＩＦ）３２と、ＬＣＤコントローラ３３と、ＬＥＤコントローラ３４と、ページ

メモリ３００を制御し、かつ、ページメモリ３００とシステムバス９上の後述するデバイスとスキャナ画像ＩＦ９２を介して接続されたスキャナサブユニット２とプリンタ画像ＩＦ９１を介して接続されたプリンタサブユニット４との間で画像データの転送を制御するＰＭ－ＣＯＮ３５を有するものである。

【００５１】

ＰＭ－ＣＯＮ３５は、ページメモリ３００をアクセスするデバイスからのアクセス要求を所定の優先度順位で調停し、順次アクセス要求に基づいてページメモリ３００をアクセスする。

【００５２】

このページメモリ３００をアクセスするデバイスとしては、スキャナ画像ＩＦ９２を介して画像データをページメモリ３００へ書き込むスキャナイメージプロセッシング部２０２、プリンタ画像ＩＦ９１を介してページメモリ３００上の画像データを読み出すプリンタイメージプロセッシング部４１、システムＣＰＵ１０、ＬＣＤコントローラ３３、ページメモリ３００上の画像データをＨＤＤ８３０へ蓄積したり又はＨＤＤ８３０に蓄積された画像データをページメモリ３００へ戻したりするＩＤＥコントローラ８００がある。

【００５３】

また、ページメモリ３００は、画像データを一時的に記憶する領域の他に、ＬＣＤ７０に表示するための表示データを記憶する表示データ領域が設けられており、ＬＣＤコントローラ３３は、周期的に表示データ領域に記憶されている表示データを読み出し、制御パネル７上のＬＣＤ７０が出力する同期信号に同期して、表示データをＬＣＤ７０へ出力する。ＬＣＤ７０は、表示データを順次表示する。

【００５４】

次に、ページメモリ３００のＰＭ－ＣＯＭ３５の内部構成について説明する。図４は、ＰＭ－ＣＯＭ３５の内部構成を示した構成図である。

【００５５】

ＰＭ－ＣＯＭ３５は、ページメモリ３００と他の処理ブロックとのデータ転送をインタフェースする転送チャネルと、データ処理ブロック（圧縮処理３５３０

及び伸長処理３５３１）と、回転処理３５３２と、各転送チャネル毎にページメモリ３０のアドレスを発生するアドレス発生部と、ＰＤＲＡＭ制御部３６とを有するものである。

【００５６】

転送チャネルは、スキャナＩＦ３５０１と、プリンタＩＦ３５０９と、ＨＤＤ転送（ｃｈ０）３５０４と、ＨＤＤ（ｃｈ１）３５０６と、圧縮（入力）３５０２と、圧縮（出力）３５０３と、伸長（入力）３５０７と、伸長（出力）３５０８と、メモリクリア３５１０と、ＣＰＵＩＦ３５１１と、ＬＣＤＩＦ３５１２とを有する。

【００５７】

また、アドレス発生部は、ＡＧＣ（ｃｈ０）３５２０と、ＡＧＣ（ｃｈ１）３５２１と、ＡＧＣ（ｃｈ２）３５２２と、ＡＧＣ（ｃｈ３）３５２３と、ＡＧＣ（ｃｈ４）３５２４と、ＡＧＣ（ｃｈ５）３５２５と、ＦＩＦＯ（ｃｈ１－Ａ）３５２６と、ＦＩＦＯ（ｃｈ１－Ｂ）３５２７と、ＦＩＦＯ（ｃｈ０－Ａ）３５２８と、ＦＩＦＯ（ｃｈ０－Ｂ）３５２９とを有する。

【００５８】

図１に戻り、スキャナサブシステム２は、少なくとも、原稿を所定のタイミングで搬送する図示しない原稿搬送部と、原稿搬送に同期して、原稿をライン単位で、光学的に読み取り電気信号に変換するＣＣＤ２０１と、ＣＣＤ２０１が出力する電気信号を所定の画素（例えば８ｂｉｔ／画素）に変換し、文字モード、文字写真モード、写真モード等指定された画像モードに適した画像処理を実行した後、１ｂｉｔ／画素のデータに階調処理し、所定のタイミングで画像データをスキャナ画像ＩＦ９２を介して、ページメモリ制御部３へ出力するスキャナイメージプロセッシング部２０２と、スキャナサブユニット２を制御するスキャナＣＰＵ２０３等を有するものである。

【００５９】

プリンタサブシステム４は、少なくとも、ページメモリ３００に一時的に記憶された画像データを、プリンタ画像ＩＦ９１を介して、所定のタイミングで読み出し、指定されたモードで画像処理するプリンタイメージプロセッシング部４１

と、プリンタイメージプロセッシング部４１からの画像データを光信号に変換するレーザドライブ回路４２と、レーザドライブ回路４２の光信号に基づいて、静電記録方式により、像を形成し、所定の用紙に転写して出力する図示しない像形成部と、プリンタサブシステム４を制御するプリンタＣＰＵ４３等を有するものである。

【００６０】

（Ａ－２）第１の実施形態の動作

以下では、第１の実施形態の画像形成装置において、画像データを暗号化に使用する暗号キーの設定入力方法の動作について図面を参照して説明する。

【００６１】

図５は、本実施形態に係る暗号キーの設定を説明するフローチャートである。

【００６２】

本実施形態の画像形成装置の画像データの暗号化に使用する機体個別の暗号キーを初期設定又は何らかの事情により暗号キーが消失した場合に、ユーザにその暗号キーのキー値の入力要求を求めるよう、ＬＣＤ７０に表示する。勿論、ＬＣＤ７０に暗号キーのキー値の入力要求の表示させることなく、ユーザの操作により設定入力を開始させるようにしてもよい。

【００６３】

タッチパネル７１又はＫｅｙ７を介して、ユーザにより暗号キーのキー値が入力される。（Ｓ１）。

【００６４】

ここで、本実施形態では、暗号キーのキー値を１６進数表示の１６桁（６４ｂｉｔ）で表示したものとする。なお、この暗号キーのキー値に所定ビット数の誤り検出符号を設けるようにしてもよい。

【００６５】

ＬＣＤ７９には、ユーザにより入力された暗号キーのキー値が表示される（Ｓ２）。図６は、入力される暗号キーのキー値の表示イメージを示す。

【００６６】

図６（Ａ）に示すように、ユーザが入力するキー値は、４桁毎に表示する。図

６（Ｂ）に示すように、ユーザが４桁のキー値が入力され、次の桁のキー値（４の倍数の次の桁のキー値）が入力されると、既に入力された前の４桁のキー値が、アスタリスク「＊」に変換された形で表示される。または、４桁のキー値の入力が終わった時点で、その４桁のキー値をアスタリスクに変形してもよい。

【００６７】

これを繰り返し、図６（Ｃ）のように、１６桁のすべてのキー値が入力されると、図６（Ｄ）に示すように、１６桁すべてのキー値がアスタリスク「＊」に変換されて表示される（Ｓ３）。

【００６８】

次に、ユーザがＳ１～Ｓ３で入力したキー値を再度入力要求をする。このとき、第１回目と同様に、４桁ずつのキー値を表示し、４桁のキー値の入力が終了し次の桁のキー値が入力されると、その前の４桁のキー値をアスタリスク「＊」に変換表示する（Ｓ４～Ｓ６）。

【００６９】

第１回目に入力されたキー値と、第２回目に入力されたキー値とが同一であるか否かが判断される（Ｓ７）。

【００７０】

その結果、第１回目と第２回目とも同一のキー値である場合には、そのキー値が暗号キーとしてＮＶＲＡＭ１４に設定される（Ｓ８）。

【００７１】

また、第１回目に入力されたキー値と、第２回目に入力されたキー値とが異なる場合には、暗号キーとして入力されたキー値に誤りがあったとして設定されない。この場合、再度ユーザに暗号キーのキー値入力を要求してもよい。

【００７２】

以上のようにして、初期設定時又は暗号キーの消失などの場合に、ユーザにより暗号キーを設定入力させることができる。

【００７３】

（Ａ）第１の実施形態の効果

以上、第１の実施形態によれば、初期設定時又は何らかの事情により画像デー

タの暗号化に使用する暗号キーを、暗号化画像データを蓄積するＨＤＤ８３０とは別の基板からなる不揮発性メモリ（ＮＶＲＡＭ１４）に記憶することにより、ＨＤＤ８３０が盗まれたとしても、ＮＶＲＡＭ１４が無事であれば、ＨＤＤ８３０の蓄積データの解読を防止することができる。

【００７４】

また、第１の実施形態によれば、ユーザによる暗号キーの設定入力を複数回行なわせ、その複数回入力された暗号キーがすべて同一のものであるか否かを判断することにより、セキュリティーを高めることができる。

【００７５】

更に、第１の実施形態によれば、ユーザにより入力させた暗号キーを所定の桁数毎にアスタリスクに変換表示することにより、第三者による盗み見を防止することができる。

【００７６】

（Ｂ）他の実施形態

（Ｂ－１）上述した実施形態は、デジタル複写装置に適用した場合について説明したが、データを暗号化し、その暗号化したデータを蓄積する蓄積装置（ＨＤＤ）を有する画像形成装置（例えばプリンタ、ファクシミリ、複合機等）に広く適用できる。

【００７７】

例えば、画像形成装置がプリンタである場合、例えば、プリンタは、ユーザが使用する端末装置（例えばパソコン等）から取り入れた画像データを受け取り、複数の用紙にプリントするような場合に、画像データを暗号化してＨＤＤに記憶してプリントする場合に適用できる。

【００７８】

また例えば、画像形成装置がファクシミリである場合、例えば、ファクシミリは、伝送されてきた情報の受信時や、送信メモリ時等に適用できる。

【００７９】

（Ｂ－２）また、画像形成装置が複合機（例えば複写機能とプリンタ機能とファクシミリ機能とを有する複合機）である場合、各機能モード毎に異なる暗号キー

を設定して使用するようにしてもよい。

【００８０】

（Ｂ－３）上述した第１の実施形態では、ユーザに入力されたキー値を４桁毎に表示し、次の桁のキー値が入力された後にその入力された４桁のキー値をアスタリスクに変換して表示することとしたが、これに限ることなく、第三者による盗み見を防止できれば、例えば、１桁のキー値が入力される毎や、又は８桁のキー値入力毎等のように適用することができる。

【００８１】

（Ｂ－４）上述した第１の実施形態では、第１回目に入力されたキー値と第２回目のキー値とが同一か否かの判断は、第２回目のキー値が入力された後に行なうこととして説明したが、これに限らず、例えば、１桁のキー値の入力毎や、又４桁毎のキー値の入力毎に同一性の判断をするようにしてもよい。

【００８２】

（Ｂ－５）上述した第１の実施形態において、暗号キーを機体個別の暗号キーであり、初期設定時又は何らかの事情により暗号キーが消失した場合に、新たに設定入力する暗号キーも、その機体個別の暗号キーであるとして説明したが、この新たに設定入力する暗号キーをユーザ独自に決定した暗号キーを適用するようにしてもよい。

【００８３】

（Ｂ－６）上述した第１の実施形態において、ＬＣＤ７０は、前回設定入力した暗号キーのキー値を表示するようにしてもよい。

【００８４】

また、上述した第１の実施形態では、キー値の入力、表示を１６進表示として説明したが、１０進表示法に従った桁表記で行なうようにしてもよい。

【００８５】

【発明の効果】

以上、第１及び第２の本発明によれば、ユーザにより入力された暗号キーのキー値を入力手段が取り込み、キー値判断手段がユーザにより予め設定された所定回数入力されたキー値が同一であるか否かの判断し、キー値判断手段が同一であ

ると判断した場合に、入力されたキー値を暗号キーとして不揮発性記憶手段に記憶することにより、暗号化に供する暗号キーの設定入力時に、ユーザにより暗号キーの設定入力が正しく行なえることができる。

【図面の簡単な説明】

【図１】　第1の実施形態の画像形成装置の全体構成ブロックを示したものである。

【図２】　第1の実施形態のシステムＣＰＵ１０の内部構成を示したブロック図である。

【図３】　第1の実施形態のページメモリ制御部３０１の内部構成を示したブロック図である。

【図４】　第1の実施形態のＰＭ－ＣＯＭ３５の内部構成を示した簿六層である。

【図５】　第1の実施形態の暗号キーの設定入力動作のフローチャートである。

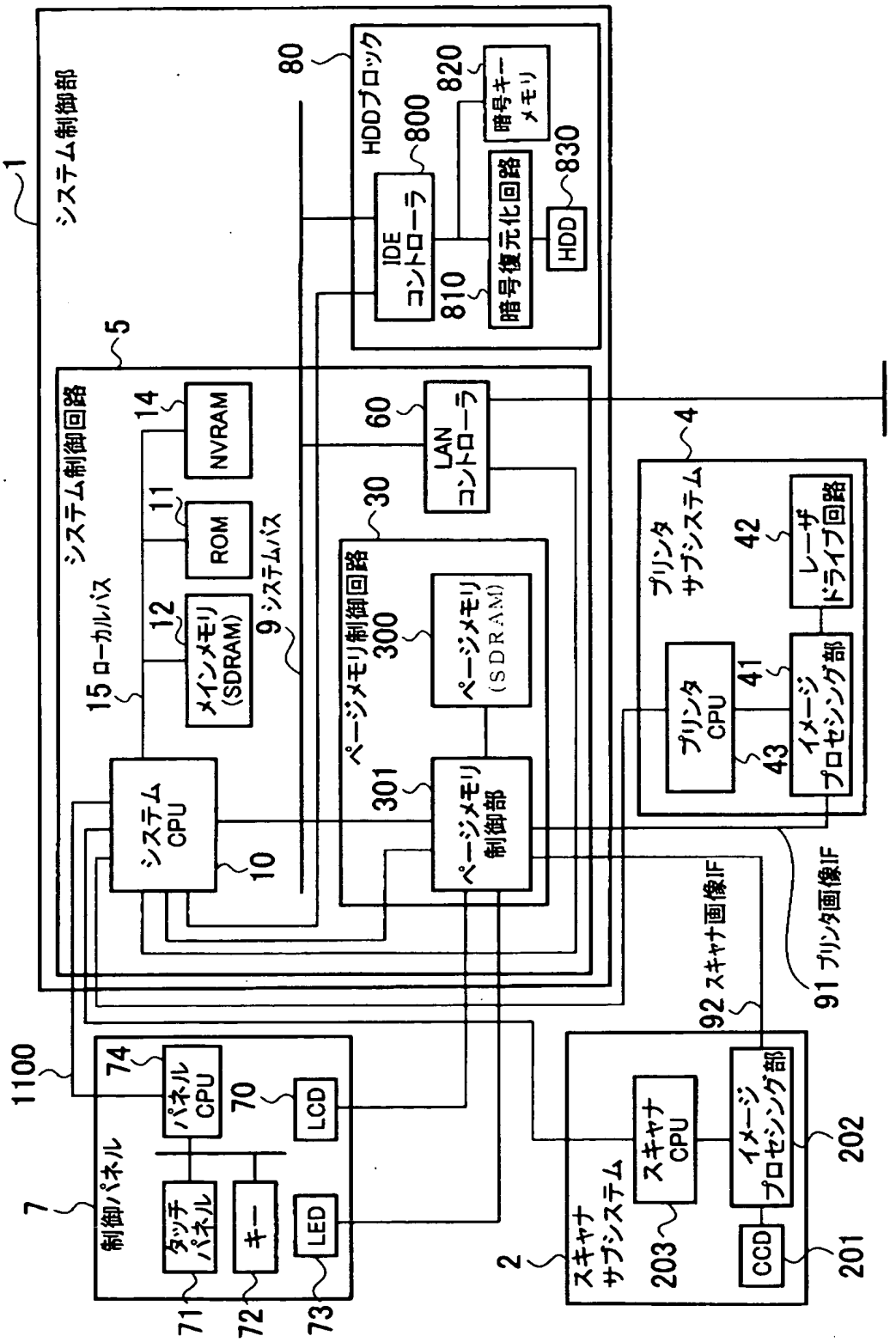
【図６】　入力される暗号キーの表示イメージを説明する説明図である。

【符号の説明】

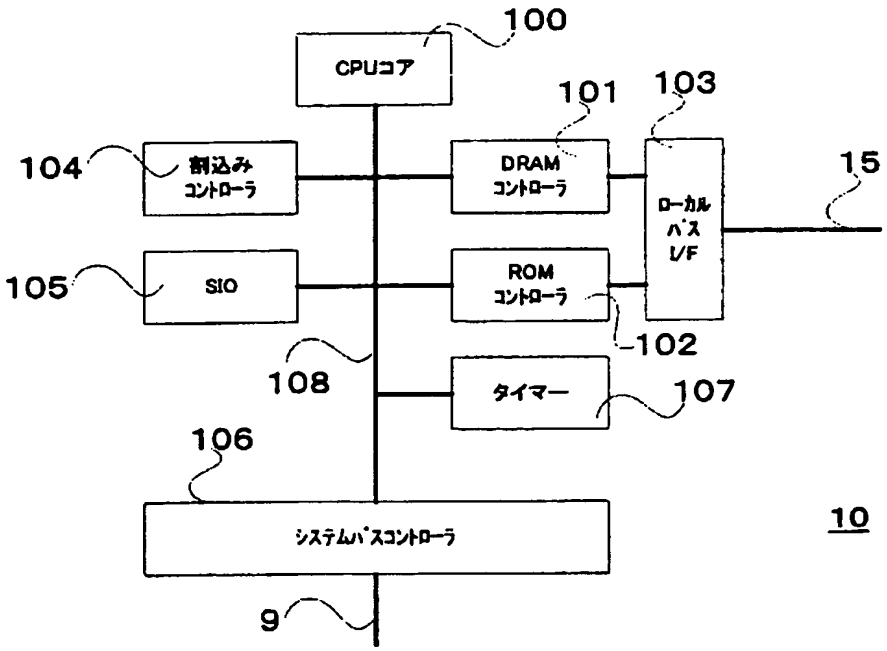
７…制御パネル、７０…ＬＣＤ、７１…タッチパネル、７２…キー、
７４…パネルＣＰＵ、１４…ＮＶＲＡＭ、８０…ＨＤＤブロック、
８１０…暗号復元化回路、８３０…ＨＤＤ、８００…ＩＤＥコントローラ。

【書類名】　図面

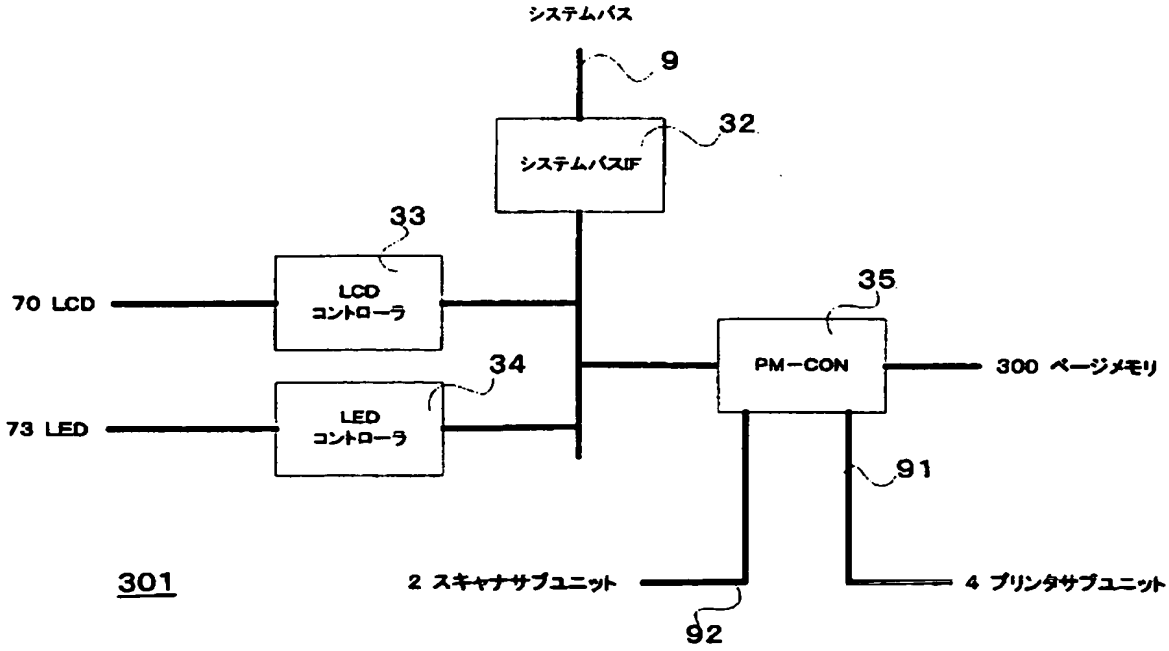
【図１】


システム制御部
1
システム制御回路
5
HDDブロック
80
IDE
コントローラ
800
暗号キー
メモリ
820
暗号復元化回路
810
HDD
830
LAN
コントローラ
60
NVRAM
14
ROM
11
メインメモリ
(SDRAM)
12
15 ローカルバス
9 システムバス
システム
CPU
10
ページメモリ制御回路
30
ページメモリ
(SDRAM)
300
ページメモリ
制御部
301
プリンタ
サブシステム
4
プリンタ
CPU
41
イメージ
プロセシング部
43
レーザ
ドライブ回路
42
91 プリンタ画像IF
92 スキャナ画像IF
制御パネル
7
1100
パネル
CPU
74
LCD
70
タッチ
パネル
71
キー
72
LED
73
スキャナ
サブシステム
2
スキャナ
CPU
203
イメージ
プロセシング部
202
CCD
201

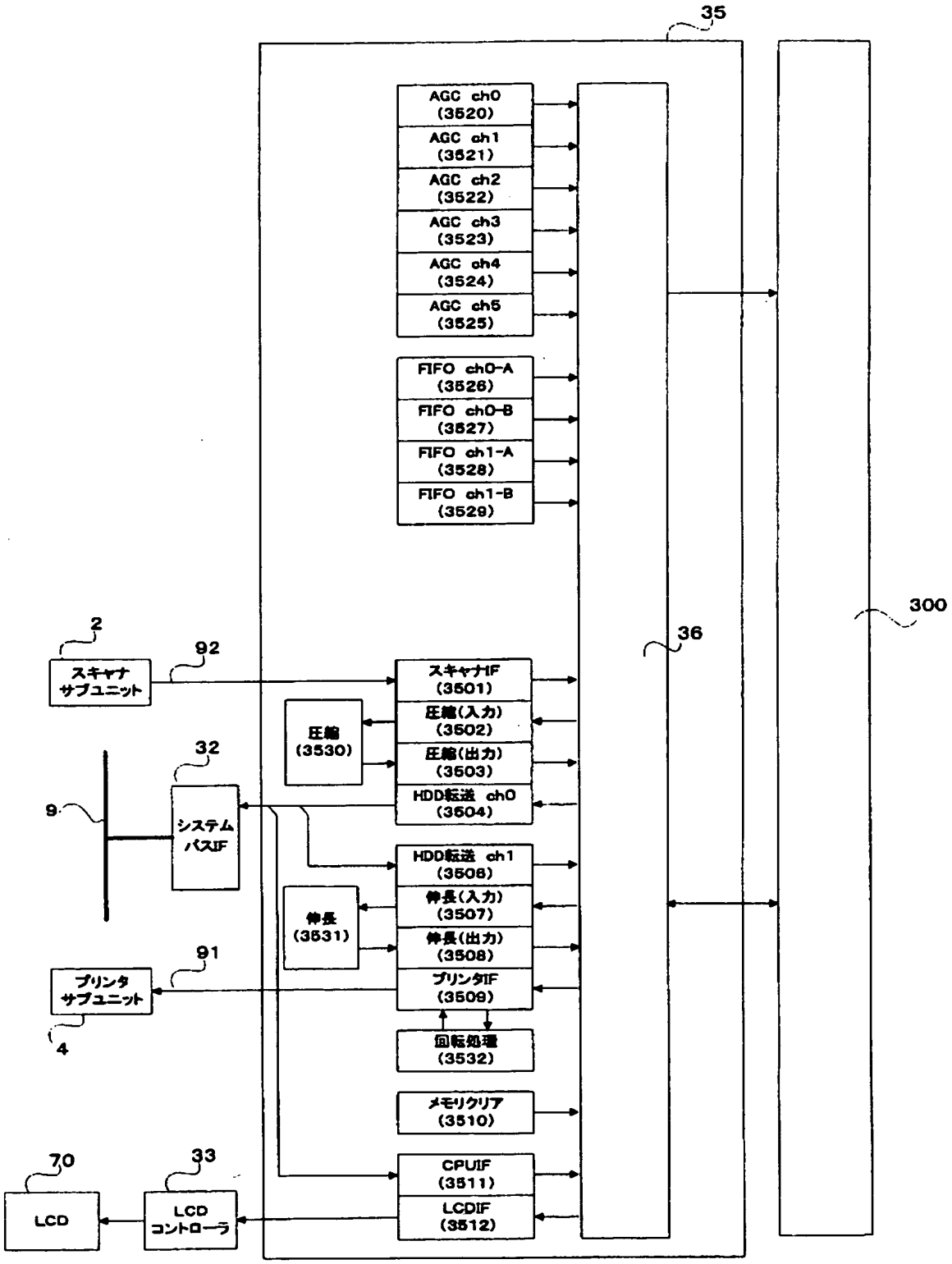
【図２】


100
CPUコア
101
103
104
割込み
コントローラ
DRAM
コントローラ
15
ローカル
バス
I/F
105
SIO
ROM
コントローラ
102
108
タイマー
107
106
システムバスコントローラ
10
9

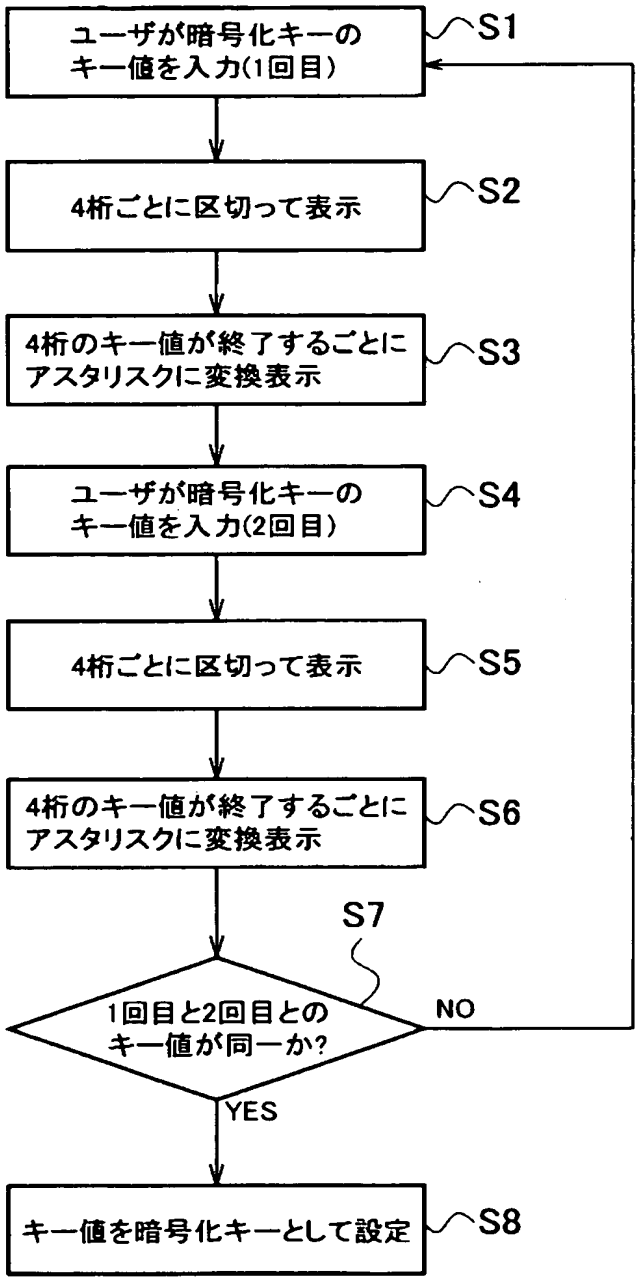
【図３】


システムバス
9
32
システムバスIF
33
70 LCD
LCD
コントローラ
35
PM−CON
300 ページメモリ
34
73 LED
LED
コントローラ
91
301
2 スキャナサブユニット
4 プリンタサブユニット
92

【図４】

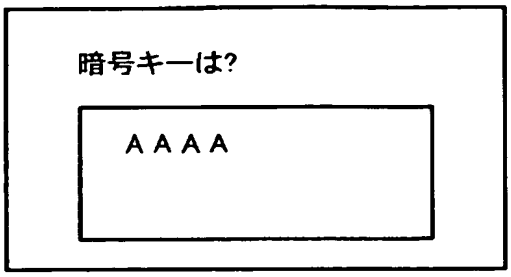

35
AGC ch0 (3520)
AGC ch1 (3521)
AGC ch2 (3522)
AGC ch3 (3523)
AGC ch4 (3524)
AGC ch5 (3525)
FIFO ch0-A (3526)
FIFO ch0-B (3527)
FIFO ch1-A (3528)
FIFO ch1-B (3529)
300
36
2
スキャナ サブユニット
92
スキャナIF (3501)
圧縮 (3530)
圧縮(入力) (3502)
圧縮(出力) (3503)
32
9
システム バスIF
HDD転送 ch0 (3504)
HDD転送 ch1 (3508)
伸長 (3531)
伸長(入力) (3507)
伸長(出力) (3508)
91
プリンタ サブユニット
4
プリンタIF (3509)
回転処理 (3532)
メモリクリア (3510)
70
33
LCD
LCD コントローラ
CPUIF (3511)
LCDIF (3512)

【図５】

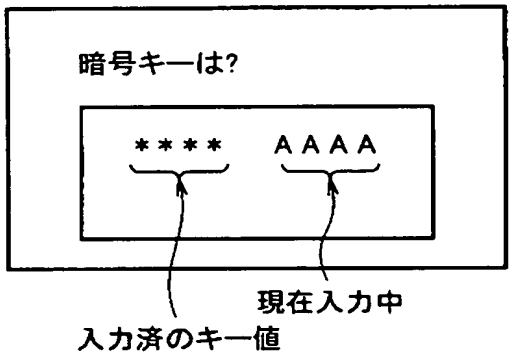

ユーザが暗号化キーのキー値を入力(1回目)
S1
4桁ごとに区切って表示
S2
4桁のキー値が終了するごとにアスタリスクに変換表示
S3
ユーザが暗号化キーのキー値を入力(2回目)
S4
4桁ごとに区切って表示
S5
4桁のキー値が終了するごとにアスタリスクに変換表示
S6
S7
1回目と2回目とのキー値が同一か?
NO
YES
キー値を暗号化キーとして設定
S8

【図６】

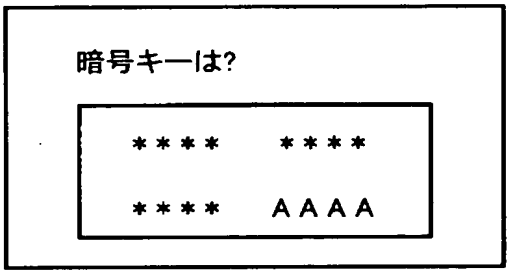
(A)



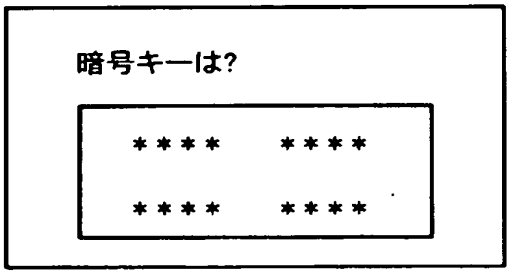
(B)



(C)



(D)



【書類名】　　要約書

【要約】

【課題】　入力画像データを暗号化して蓄積する際に、暗号化に供する暗号キーの設定入力時に、ユーザにより暗号キーの設定が正しく行なえ得る暗号キー設定入力方法と、画像形成装置とを提供する。

【解決手段】　本発明の暗号キー設定入力方法は、ユーザにより入力された暗号キーのキー値を入力手段が取り込み、キー値判断手段がユーザにより予め設定された所定回数入力されたキー値が同一であるか否かの判断し、キー値判断手段が同一であると判断した場合に、入力されたキー値を暗号キーとして不揮発性記憶手段に記憶することを特徴とする。

【選択図】　　図１

【書類名】　出願人名義変更届
【整理番号】　TEC067M
【提出日】　平成15年12月 4日
【あて先】　特許庁長官　今井　康夫　殿
【事件の表示】
　【出願番号】　特願2003- 53145
【承継人】
　【識別番号】　000003078
　【氏名又は名称】　株式会社東芝
　【代表者】　岡村　正
【承継人代理人】
　【識別番号】　100090620
　【弁理士】
　【氏名又は名称】　工藤　宣幸
　【電話番号】　03(3981)8899
【手数料の表示】
　【予納台帳番号】　013664
　【納付金額】　4,200円
【提出物件の目録】
　【物件名】　一部譲渡証書　1
　【提出物件の特記事項】　手続補足書により提出する
　【物件名】　株式会社東芝の委任状　1
　【提出物件の特記事項】　手続補足書により提出する
　【包括委任状番号】　0107421

認定・付加情報

特許出願の番号	特願２００３－０５３１４５
受付番号	５０３０２００１５９２
書類名	出願人名義変更届
担当官	伊藤　雅美　　２１３２
作成日	平成１６年　１月１９日

＜認定情報・付加情報＞

【承継人】

【識別番号】　000003078

【住所又は居所】　東京都港区芝浦一丁目１番１号

【氏名又は名称】　株式会社東芝

【承継人代理人】　申請人

【識別番号】　100090620

【住所又は居所】　東京都豊島区南池袋２丁目４１番８号　池袋睦ビル２階　工藤特許事務所

【氏名又は名称】　工藤　宣幸

特願２００３－０５３１４５

出　願　人　履　歴　情　報

識別番号　　［０００００３５６２］

１．変更年月日　　１９９９年　１月１４日
［変更理由］　　名称変更
住所変更
住　所　　東京都千代田区神田錦町１丁目１番地
氏　名　　東芝テック株式会社

特願２００３－０５３１４５

出願人履歴情報

識別番号　［０００００３０７８］

１．変更年月日　２００１年　７月　２日
［変更理由］　住所変更
住　所　東京都港区芝浦一丁目１番１号
氏　名　株式会社東芝